Indian Union (IU) Data Protection Law- What does it convey?

Data protection law in India is currently facing many problem and resentments due the absence of proper legislative framework. There is an ongoing explosion of cyber crimes on a global scale. The theft and sale of stolen data is happening across vast continents where physical boundaries pose no restriction or seem non-existent in this technological era. India being the largest host of outsourced data processing in the world could become the epicenter of cyber crimes this is mainly due absence of the appropriate legislation. The Data Security Council of India (DSCI) and Department of Information Technology (DIT) must also rejuvenate its efforts in this regard on the similar lines. However, the best solution can come from good legislative provisions along with suitable public and employee awareness. It is high time that we must pay attention to Data Security in India. Cyber Security in India is missing and the same requires rejuvenation. When even PMO's cyber security is compromised for many months we must at least now wake up. Data breaches and cyber crimes in India cannot be reduced until we make strong cyber laws. We cannot do so by mere declaring a cat as a tiger. Cyber law of India must also be supported by sound cyber security and effective cyber forensics.

Indian companies in the IT and BPO sectors handle and have access to all kinds of sensitive and personal data of individuals across the world, including their credit card details, financial information and even their medical history. These Companies store confidential data and information in electronic form and this could be vulnerable in the hands of their employees. It is often misused by unsurplous elements among them. There have been instances of security breaches and data leakages in high profile Indian companies. The recent incidents of data thefts in the BPO industry have raised concerns about data privacy.

There is no express legislation in India dealing with data protection. Although the Personal Data Protection Bill was introduced in Parliament in 2006, it is yet to see the light of day. The bill seems to proceed on the general framework of the European Union Data Privacy Directive, 1996. It follows a comprehensive model with the bill aiming to govern the collection, processing and distribution of personal data. It is important to note that the applicability of the bill is limited to ‘personal data’ as defined in Clause 2 of the bill.

The bill applies both to government as well as private enterprises engaged in data functions. There is a provision for the appointment of, “Data Controllers”, who have general superintendence and adjudicatory jurisdiction over subjects covered by the bill. It also provides that penal sanctions may be imposed on offenders in addition to compensation for damages to victims.

The bill is clearly a step in the right direction. However due to the paucity of information, the bill is still pending.

While the Information Technology Act, 2000 (IT Act), contains provisions regarding cyber and related IT laws in India and delineates the scope of access that a party may have to on data stored on a computer, computer system or computer network, the provisions of the IT Act do not address the need for a stringent data protection law being in place.

The Information Technology Act, 2000 has recently been amended to meet challenges in cyber crime, the amended Act is yet to come into force, it has introduced two important provisions that have a strong bearing on the legal regime for data protection. These are sections 43A and 72A, inserted into the IT Act by the amendment Act. But the provisions pertaining to data security and confidentiality are grossly inadequate. In recent years the incidents of data theft in BPO has raised concern about the data privacy when one of its employees sold personal data belonging to a large number of British nationals to an undercover reporter from the British tabloid ‘The Sun’. The incident sparked off a debate among the offshore industry circles, media and the legal world as to how safe foreign data is in Indian hands. Hence, the amendments, are more of a knee-jerk reaction from the Government to the recent data thefts and other incidents, India has more to do with issues related to cyber crimes and e-commerce transactions than data protection.

The provisions purportedly for ‘data protection’ jut out as an ugly patch work on the IT Act and do not offer any comprehensive protection to personal data in India. In these circumstances the question to be asked is, Being a major IT power in the global map today, can India afford to deal with an important issue such as this in the manner in which it has dealt with in the amendments to the IT Act?.

The Recent amendments to IT Act are

Section 43A states that if a “body corporate” possessing, dealing or handling any “sensitive personal data or information” in a computer resource which it owns, controls or operates is negligent in implementing and maintaining “reasonable security practices and procedures”, and thereby causes

wrongful loss or wrongful gain to any person, this body corporate will become liable to pay damages as compensation to the affected person.

The term “body corporate” is wide enough to include a company, a firm, sole proprietorship or other association of individuals engaged in professional or commercial activities. And then regarding “reasonable security practices and procedures include security practices and procedures desiring to protect information unauthorised damage, use, modification, disclosure or impairment as may be specified either

(i) in an agreement between the parties; or

(ii) in any law in force; and in the absence of an agreement or law, as may be prescribed by the Union government,

This mainly means that the contracting parties may specify in their contract the extent of security they demand from the disclosing parties in case of breach they are liable to pay the damages.

However, the amendment Act has not specified the meaning of the term “sensitive personal data or information” and merely states that it would mean such personal information as may be prescribed by the Union government in consultation with such professional bodies or associations as it may deem fit.

Section 72 is limited to information being obtained by virtue of a “power granted under the IT Act”. The purview of section 72A, on the other hand, is wider than the existing section 72 and extends to disclosure of personal information of a person (without consent) while providing services under a lawful contract and not merely disclosure of information obtained by virtue of “powers granted under the IT Act”.

The term “intermediary” is added to section72A. This has been defined under the amendment Act to mean (with respect to any particular electronic record) a person, who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, Internet service providers, Web-hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes.

On comparing the Indian law with the law of developed countries the proper requirement for the Indian law can be analysed. U.K. has its Data Protection Act (DPA) of 1998. This Act is basically instituted for the purpose of providing protection and privacy of the personal data of the individuals in UK.

According to this Act , the persons and organizations which store personal data must register with the information commissioner, which has been appointed as the government official to oversee the Act. The Act put restrictions on collection of data. Personal data can be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes. The personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.

Both U.S and the European Union focus on enhancing privacy protection of their citizens, U.S takes a different approach to privacy from that of the European Union. US adopted the sectoral approach that relies of mix of legislation, regulation, and self regulation. In U.S, data are grouped into several classes on the basis of their utility and importance. Thereafter, accordingly a different degree of protection is awarded to the different classes of data. Whereas the provisions of IT Act deal basically with extraction of data, destruction of data, etc. Companies cannot get full protection of data through that which ultimately forced them to enter into separate private contracts to keep their data secured. These contracts have the same enforceability as the general contract.

The European Union has enforced a comprehensive Directive on Protection of personal Data to all its member countries. The US has also complied with the EU directive through the Safe Harbour Agreement to facilitate business from the EU countries. It would be wise for India to comply with the EU directive as well, as it has a lot at stake.

Despite the efforts being made for having a data protection law as a separate discipline, our legislature have left some lacuna in framing the bill of 2006. The bill has been drafted wholly on the structure of the UK Data Protection Act whereas today's requirement is of a comprehensive Act. Thus it can be suggested that a compiled drafting on the basis of US laws relating to data protection would be more favourable to the today' requirement.

Unauthorised use or transfer of this credit data attracts prohibitive fines. Credit information can be used only to identify the credit worthiness of a potential customer and cannot be used or transferred to unauthorised persons for any other purpose. The IT Act again, protects credit data exclusively which is just one aspect of personal data.

Any piecemeal legislation is insufficient; we need comprehensive data protection legislation that will protect the rights of data subjects, that will vehemently prohibit the use of collected data for any purpose other than for which it has been. The Information Technology Act, 2000 is not data or privacy protection legislation perse. It does not lay down any specific data protection or privacy principles. The Information Technology Act, 2000 is a generic legislation, which articulates on range of themes, like digital signatures, public key infrastructure, e-governance, cyber contraventions, cyber offences and confidentiality and privacy. It suffers from a one Act syndrome. It would be erroneous to compare the Information Technology Act, 2000 provisions with the European Directive on Data Protection (EC/95/46), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980, and the Safe Harbor principles of the US.

In fact the Information Technology Act, 2000 deals with the issue of data protection and privacy in a piecemeal fashion. There is no an actual legal framework in the form of Data Protection Authority, data quality and proportionality, data transparency etc. which properly addresses and covers data protection issues in accordance with the principles of the EU Directive, OECD Guidelines or Safe Harbor Principles. Accordingly, even if the new proposed amendments to the Information Technology Act, 2000 were adopted, India would still lack a real legal framework for data protection and privacy.

Absence of the Data protection law is huge blow to outsourcing industry in India . The US, European Union customers are protected by a comprehensive privacy Directive, and part of that privacy protection is the requirement, placed on companies, not to transfer personal data to countries which do not offer an adequate level of protection. The result is that European Trades Unions have cited data protection as an issue which should be taken into account in many international out-sourcing deals. Stop the flow of personal data, which in turn will affect our outsourcing industry very badly.

Conclusion

For sustaining and encouraging the BPO boom, India needs to have a legal framework that meets with the expectations, both legal and of a public nature, as prevail in the jurisdictions from which data is being shipped to India. In practical terms the biggest hurdle is for India to have its framework of domestic data protection laws officially adjudged and publicly perceived as “adequate”. The EU officially declares and lists ‘adequate’ countries in terms of its 1995 Data Protection Directive. Only a handful of countries like Argentina, Canada, Australia and Switzerland, have so far made it to this “white list.” If India were also to make it to this list by enacting a suitable legislation, industries within the EU Member

states would be able to export data to India without having to follow otherwise compulsory difficult and cumbersome procedures.

India rather than limit itself to being a supplier of services to corporate America and Europe, India sees itself as the place where such corporations can establish themselves. Thus by creating a good data protection law India could extend well beyond being a mere supplier of services to the world's multi-national corporations. In effect, it wants to establish corporate India.